



(11)

EP 3 800 911 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:

27.03.2024 Bulletin 2024/13

(51) International Patent Classification (IPC):

H04W 12/02 ^(2009.01) **H04W 12/00** ^(2021.01)
H04W 12/033 ^(2021.01) **G06Q 20/36** ^(2012.01)
G06F 21/62 ^(2013.01) **G07G 1/01** ^(2006.01)

(21) Application number: **20192308.3**

(52) Cooperative Patent Classification (CPC):

(22) Date of filing: **24.08.2020**

H04W 12/033; G06F 21/6245; G06Q 20/36;
G07G 1/01; H04W 12/02

(54) **PRIVACY-SECURE EDGE-ZONE DIGITAL IDENTITY COMPUTING FOR OPEN-LOOP
PIXEL-STATE CONTROL**

DATENSCHUTZGERECHTE DIGITALE IDENTITÄTSBERECHNUNG IN DER RANDZONE ZUR
STEUERUNG DES PIXELZUSTANDS IN EINEM OFFENEN REGELKREIS

CALCUL D'IDENTITÉ NUMÉRIQUE À CONFIDENTIALITÉ SÉCURISÉE EN ZONE PÉRIPHÉRIQUE
POUR UN CONTRÔLE D'ÉTAT DE PIXELS EN BOUCLE OUVERTE

(84) Designated Contracting States:

**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

- **GIORDANO, Giuseppe**
4 Dublin (IE)
- **SCHIATTI, Luca**
4 Dublin (IE)
- **MILAZZO, Andrea Maria**
4 Dublin (IE)
- **PAOLINO, Dominic**
4 Dublin (IE)

(30) Priority: **03.10.2019 US 201962910079 P**
22.05.2020 US 202016881989

(43) Date of publication of application:
07.04.2021 Bulletin 2021/14

(74) Representative: **Boult Wade Tennant LLP**
Salisbury Square House
8 Salisbury Square
London EC4Y 8AP (GB)

(73) Proprietor: **Accenture Global Solutions Limited**
Dublin 4 (IE)

(72) Inventors:

- **TREAT, David B**
4 Dublin (IE)
- **KUHRT, Tracy Ann**
4 Dublin (IE)

(56) References cited:
AU-A1- 2012 223 415 US-A1- 2016 006 754
US-A1- 2017 039 389

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description**Priority**

[0001] This application claims priority to U.S. Patent Application No. 16/881,989, filed 22 May 2020, Attorney Docket No. 15718-678, entitled Privacy-Secure Edge-Zone Digital Identity Edge Computing for Open-Loop Pixel-State Control. This application also claims priority to U.S. Provisional Patent Application No. 62/910,079, filed 3 October 2019, Attorney Docket No. 15718-652, entitled Digital Identity Edge Computing.

Technical Field

[0002] This disclosure relates to edge-zone digital identity computing.

Background

[0003] Rapid advances in electronics and communication technologies, driven by immense customer demand, have resulted in the widespread adoption of electronic transactions, record keeping, and data sharing. As one example, electronically stored and tracked identity information has provided the underpinning for Big Data technologies and enterprises. Improvements in tracking and/or knowledge management attached to such electronically stored and tracked identity information will continue to increase the features and options available to operators engaging in data operations.

[0004] US 2017/0039389 A1 discusses privacy enforcement via localized personalization.

[0005] US 2016/0006754 A1 discusses a computing system including an enclave or other similar secured memory location or process.

[0006] WO 2012/118870 A1 discusses secure anonymous transaction apparatuses, methods and systems ("SAT") that transform hardware-verified user authentication requests via SAT components into secure transaction notifications.

BRIEF DESCRIPTION OF THE DRAWINGS**[0007]**

Figure 1 shows an example pixel-state control environment.

Figure 2 shows example control prime logic.

Figure 3 shows an example control prime execution environment.

Figure 4 shows an example edge-zone device.

Figure 5 shows an example ladder diagram for an example system with a physically-localized edge-zone.

Figure 6 shows an example ladder diagram for an example system with a logically-localized edge-zone.

DETAILED DESCRIPTION

[0008] In an electrical and computer system, a central control system may control one or more functions on a target device. In some cases, the control decisions may be based on feedback data sent from the target device back the central control system allowing the central system to adjust control parameters to reflect information collected at the target device, for example, local sensor data, and not necessarily locally-available to the central control system. Thus, the system operates in an open-loop control state.

[0009] In an example open-loop pixel state control system, a display control prime (e.g., a central display state control system) may control pixel-states (e.g., on-off states, color states, brightness states or other physical real-world states of one or more pixels) making up at least a portion of a display on an edge-zone device (e.g., such as a mobile device within an edge-zone, as discussed below). For example, a display control prime may cause a set of pixel-states that result in an interactive display (e.g., a dialogue box, an information window, an emergency alert, a commercial offer, opportunity for automated service requests, or other interactive display) being presented.

[0010] In some cases, data on which the display control prime may base a pixel-state control determination on sensitive data (e.g., un-sanitized data, as discussed below). Accordingly, transferring the sensitive data to the display control prime may constitute a violation of privacy and/or security standards. To allow the display control prime to effect open-loop control, the display control prime may cause/provide for provisioning of an agent to run on the controlled device (or otherwise within a privacy-secure edge-zone). By providing a pixel-state control parameter matrix supporting conditional pixel-state commands, the provisioned agent may handle computations on sensitive data from within a privacy-secure edge-zone. This leaves the display control prime blind to (e.g., unable to view) the sensitive data, but still allows for prime-blind open-loop pixel-state control. Thus, the provisioned agent may handle analysis of sensitive data from within the edge-zone in the display control prime's stead.

[0011] The techniques and architectures discussed herein (including edge-zone enforcement, provisioned agents, sanitized uplink establishment, and/or control prime circuitry) provide a technical solution (e.g., digital edge computing execution and support) to a technical problem (e.g., execution of open-loop pixel-state control without sensitive data portability) thereby improving the operation of the underlying hardware. Further, because the techniques and architectures discussed herein (including edge-zone enforcement, provisioned agents, sanitized uplink establishment, and/or control prime circuitry) allow for increased compartmentalization of data, these techniques and architectures also increase the security of the computer and computing systems on which

these techniques and architectures are implemented. Further, the increased privacy afforded by these techniques and architectures provide an improvement over existing market-based solutions.

[0012] In various implementations, securing data within a defined edge-zone allows for access to data (which may include sensitive private data) from which to base pixel-state commands. In various systems, similar data may be derived using various analytic tools (which may be computationally intensive, in some cases) from data available outside the edge-zone. In other words, in some cases, the data used in the pixel-state calculations may, in some cases, be computationally predicted or derived rather than obtained from the user from which it originates. However, such analytic derivation may have comparatively less accurate and efficient than a direct poll of the source of the data. Accordingly, establishment and enforcement of the edge-zone may increase the accuracy and efficiency of the underlying hardware performing the open-loop pixel-state control.

[0013] In various implementations, data sharing control may be implemented by applying homomorphic encryption (e.g., a cryptologic technique) to un-sanitized data. The homomorphic encryption may allow sharing of selected data, data details, metadata, and/or other data features without necessarily sharing un-sanitized data from which such selected data features may be derived or later recreated. The un-sanitized data may refer to data in a decrypted / unencrypted form on which pixel-control state determinations may be made. For example, un-sanitized data may include empirical data, test data, survey data, collected data, historical utilization data, sales data environmental data, industrial data, fabrication specifications, identity data, credit-worthiness data, educational credential data, government record data, or other data on which analyses may be performed.

[0014] Homomorphic encryption schemes may include a class of multiple different encryption schemes. Homomorphic encryption schemes use a homomorphic property of certain encryption algorithms, e.g., $H_m(x)$, where H_m designates a homomorphic encryption algorithm. The homomorphic property provides that the sum of encrypted values is equal to the value of the encrypted sum of the values, e.g., $H_m(x) + H_m(y) = H_m(x+y)$. This homomorphic property may be used to disclose various features of the underlying data values, e.g., x and y , without disclosing x and y , using various known mathematical results from the homomorphic property. Further, because addition (e.g., an ADD operation) and multiplication (e.g., a MULT operation) may be performed on the encrypted data without decryption, processing operations, such as mathematical or modeling operations, may be performed on the data while in an encrypted state. Similarly, subtraction operations may be performed (e.g., inverse additions because: $H_m(x+y) + - H_m(y) = H_m(x)$). Accordingly, insights may be gleaned from aggregated data and/or sanitized data (e.g., privacy-preserving selected information) regarding without disclosing the un-

sanitized data.

[0015] In some cases, homomorphic encryption and/or other encryption schemes may be implemented to enforce logical zones, as discussed below. In some cases, the logical zones may be implemented as secure enclaves that are local to a device (such as an edge-zone device, discussed below). The secure enclaves may offer controlled access to data for determination of actions within an open-loop pixel-state control system.

[0016] In some cases, the controlled access to the secure enclave may include access to homomorphically-encrypted data to allow manipulation and calculation without necessarily exposing private data. For example, a secure enclave may provide access to a homomorphically-encrypted version of private data, but not the underlying private data. An agent (discussed below) may execute calculation/manipulation on the homomorphically-encrypted data while encrypted. Secure local logic on the device may cause the enclave to expose an unencrypted form of the result (or execute/request a corresponding action without necessarily exposing the result) after manipulation. Thus, the underlying data remains protected within the secure enclave (and local to the device) without exposure to agent logic (including some cases where the agent itself is localized).

[0017] Additionally or alternatively, the controlled access to the secure enclave may include access to data with types of encryption that may not necessarily allow operations on the data while in an encrypted form. The enclaves may be the logical zones (which are also physically localized to specific locations on the mobile device) in which private data may be decrypted. Outside the enclave, only encrypted forms of the data may be allowed. The enclaves may be data specific, application specific, or specific to neither. For example, a particular enclave may house specified private data (photos, contacts, demographic data, financial data, and/or other private data) and mediate access to that data for applications (in some cases all applications) accessing the specified data. In some cases, enclaves may house various unspecified private data for interaction with a specific application or applications. In some cases, the enclave may mediate interactions among unspecified private data and unspecified applications.

[0018] To maintain data privacy and security, an edge-zone may be defined for an open-loop pixel-state control system. The edge-zone may be protected such that data traveling out of the edge-zone (e.g., on uplinks to the display control prime) is sanitized. The edge-zone may be logically- and/or physically-localized.

[0019] Logical localization may be defined by a logical perimeter (e.g., various physical storage and process locations that enforce the encryption requirements of the logically-localized edge-zone) which may not necessarily be physically localized. In other words, storage and processing locations within a logically-localized edge-zone may be physically distributed (in some cases, co-located (at least in part) with display control prime hard-

ware) but logically maintain the edge-zone through encryption parameters. For example, homomorphic encryption may be a condition of an example logically-localized edge-zone, but the hardware hosting processing and storage locations with example edge-zone may be physically distributed.

[0020] Physical localization may be defined by one or more physical perimeters. For example, specific hardware devices may be wholly (or partially) within the edge-zone. Thus, processing or storage on those devices would be in the edge-zone.

[0021] In some cases, an edge-zone may use physical and logical localization. For example, a physical perimeter and a logical perimeter may be defined for an edge-zone. Storage and/or processing may be in the edge-zone if it occurs within at least one of the perimeters. In some cases, both physical and logical localization may be used in tandem. Accordingly, storage and/or processing may be in the edge-zone if it occurs within both of the perimeters.

[0022] An edge-zone device may include a device (or a portion of a device) hosting storage and/or processing within an edge-zone. An edge-zone device may include a display with one or more pixels subject to pixel-state control by the display control prime.

[0023] A central-zone may include one or more regions outside the edge-zone including hardware implementing the display control prime.

[0024] Figure 1 shows an example pixel-state control environment 100. In the example pixel-state control environment 100, a display control prime 112 within a central-zone 110 has established a sanitized uplink 114 with an edge-zone provisioned agent 134 on an edge-zone device 132 in a privacy-secure edge-zone 130. In this illustrative example, the display control prime has also established an edge-support downlink 116. The display control prime 112 has provided the provisioned agent with a pixel-state control parameter matrix 118. The provisioned agent is further located within a portfolio container 140 on the edge-zone device 132. The portfolio container 140 may include a quarantined space for one or more agents (potentially controlled by multiple different prime systems). The portfolio container 140 may include an un-sanitized data import channel 142 for moving un-sanitized data from edge-zone memory 136 into the portfolio container and on to the agent(s) therein.

[0025] In some cases, prior to provisioning, pre-provisioned agents may be maintained in agent repository 150. The agent repository 150 may include multiple different pre-provisioned agents 152 corresponding to different display control prime systems (e.g., and different enterprises). Accordingly, the agent repository may be maintained by a third party controlling neither the edge-zone device 132 nor the display control prime 112. In some cases, the agent repository may include a search function and/or a virtual "app store" type storefront where users may find and install agents for their edge-zone devices. In some cases, the agents may be pre-provisioned

with the repository with the pixel-state control parameter matrix 118,

[0026] Referring now to Figure 2 while continuing to refer to Figure 1, Figure 2 shows example control prime logic (CPL) 200 which may define the operation of hardware executing as control prime circuitry.

[0027] The CPL 200 may provide a pixel-state control parameter matrix 118 to the provisioned agent 134 (202). The pixel-state control parameter matrix may include a data structure (such as a table, self-executing code, machine-learning code, or other data structure) that may accept input data (e.g., un-sanitized data available within the privacy secure edge-zone) and to identify one or more conditional pixel-state commands included within the pixel-state control parameter matrix. The conditional pixel-state commands may include details of display content that may be presented on a display of the edge-zone device (e.g., thereby controlling the pixel-states of the device). The conditionality of the commands informs the agent the conditions under which a particular conditional pixel-state command is in force (e.g., is an operative pixel-state command). In other words, the display control prime sends the conditional pixel-state commands as a group in the pixel-state control parameter matrix 118, but the display control prime is blind to the un-sanitized data on which the conditionality of the commands rests. Therefore, the agent determines which of the commands from the display control prime is in effect, by applying the un-sanitized data to the pixel-state control parameter matrix 118 and determining a conditional pixel-state command that matches the conditions.

[0028] The CPL 200 may receive sanitized feedback from the provisioned agent 134 over the sanitized uplink (204). The reception of this feedback may be dependent on the execution of provisioned agent logic (PAL) 250 by the agent. Accordingly, the execution of the PAL 250 by the agent may not necessarily be affirmatively performed by (or under the direct control of) the CPL 200 (or any entity controlling the CPL 200). Rather the execution of the PAL 250 performed by the provisioned agent describes the specific conditions under which sanitized feedback may be received by the CPL 200 over the sanitized uplink.

[0029] Referring now to the PAL 250 of Figure 2, prior to sending the sanitized feedback to the CPL 200, the PAL 250 may access un-sanitized data while the provisioned agent 134 is localized in the privacy-secure edge-zone (252). In some cases, the provisioned agent may be located within a portfolio container 140. To access the un-sanitized data from within the portfolio container 140, the provisioned agent 134 may request import of the un-sanitized data over the import channel 142.

[0030] The portfolio container 140 may enforce import rules. For example, specific agents within the portfolio container may have specifically-defined access to specific types of un-sanitized data. The portfolio container 140 (e.g., via the import channel 142) may inspect data incoming into the portfolio container (e.g., to ensure the

import rules are followed). For example, an agent maintaining pixel-state displays related to automated hotel bookings may have access to location information from the edge-zone device, but be barred from requesting educational credential information.

[0031] In some cases, provisioned agents may comply with a pre-access condition be accessing un-sanitized data. For example, the import channel 142 may constrain access to a particular type of un-sanitized data to agents that have implemented a predetermined level of encryption protection. In an example, the import channel 142 may enforce a sanitization criterion on data bound for the sanitized uplink. In the example, the import channel may force the agent to comply with a new or stricter sanitization scheme (e.g. further constraining the type data that may be sent to the display control prime) before agreeing to send additional un-sanitized data.

[0032] In some cases, provisioned agents may complete a remunerative transaction to a user of the edge-zone device before gaining access to un-sanitized data. In some cases, such rules or transactions may transform un-sanitized data into sanitized data for a provisioned agent or group of agents. However, the transformation may be constrained. For example, the transformed un-sanitized data may remain un-sanitized data for agents other than a specific agent or group of agents for which the transformation applies.

[0033] Based on the accessed un-sanitized data and the pixel-state control parameter matrix 118, the PAL 250 may identify an operative pixel-state command from among the conditional pixel-state commands in the pixel-state control parameter matrix 118 (254). Based on the operative pixel-state command, the PAL 250 may cause a change to a pixel-state of the edge-zone device 132. For example, the PAL 250 may cause a change to the physical state of pixels on the edge-zone device to display specific content on the display or a portion of the display.

[0034] Responsive to the changed pixel-state, the PAL 250 may receive raw feedback from a user interface of the edge-zone device (256). The raw feedback may include user taps or button presses or other interface device (e.g., such as those of user interface 418, discussed below). Further, the raw feedback may include or be connected to un-sanitized data. Accordingly, PAL 250 may sanitize (e.g., remove un-sanitized data) the raw feedback (258) before sending sanitized feedback to the CPL 200 over the sanitized uplink (260).

[0035] Referring again to the CPL 200 of Figure 2, the CPL 200 may send an unconditional pixel-state command based on the sanitized feedback (206). This unconditional pixel-state command may be analogous (at least in part) to corrective adjustments based on a feedback loop in open-loop control systems. For example, the unconditional pixel-state command may provide an adjustment to a previous display leading to negative sanitized feedback (e.g., updating the display with an updated more attractive promotion). In an example, the uncon-

ditional pixel-state command may include a command to display a confirmation or acknowledgment after positive sanitized feedback is received.

[0036] Figure 3 shows an example control prime execution environment (CPEE) 300 which may be implemented as control prime circuitry. The CPEE 300 may include system logic 314 to support tasks described in the disclosure, such as agent control and communication. The system logic 314 may include processors 316, memory 320, and/or other circuitry, which may be used to implement CPL 200, which may provide software support to implement the various tasks performed by the CPL 200 (e.g., to transform the CPEE 300 (at least in part) into specialized control prime circuitry). In various implementations, the CPEE 300 may include a mobile device.

[0037] The memory 320 may be used to store parameters 322 and/or model templates 324 used in the agent control and communication. The memory 320 may further store rules 321 that may facilitate agent control and communication and/or the execution of other tasks.

[0038] The memory 320 may further include applications and structures, for example, coded objects, templates, or one or more other data structures to facilitate such as agent control and communication and/or the execution of other tasks. The CPEE 300 may also include one or more communication interfaces 312, which may support wireless, e.g. Bluetooth, Wi-Fi, WLAN, cellular (3G, 4G, LTE/A), and/or wired, ethernet, Gigabit ethernet, optical networking protocols. The communication interface 312 may support communication, e.g., through the communication layer as network interface circuitry, with data sources or resources used to facilitate, such as agent control and communication and/or the execution of other tasks. Additionally or alternatively, the communication interface 312 may support secure information exchanges, such as secure socket layer (SSL) or public-key encryption-based protocols for sending and receiving sanitized and/or un-sanitized data. The CPEE 300 may include power management circuitry 334 and one or more input interfaces 328.

[0039] The CPEE 300 may also include a user interface 318 that may include man-machine interfaces and/or graphical user interfaces (GUI). The GUI may be used to present interfaces and/or options to facilitate agent and/or frontend management and/or the execution of other tasks.

[0040] Figure 4 shows an example edge-zone device 132. The example edge-zone device 132 may communicate with a basestation 402 over a wireless channel 454. In this example, the example edge-zone device 132 supports one or more Subscriber Identity Modules (SIMs), such as the SIM1 402. Electrical and physical interface 406 connects SIM1 202 to the rest of the user equipment hardware, for example, through the system bus 410.

[0041] The example edge-zone device 132 includes communication interfaces 412, system logic 414, and a

user interface 418. The system logic 414 may include circuitry and/or hardware, which may host combinations of software, firmware, or other executable code. The system logic 414 may be implemented, for example, with one or more systems on a chip (SoC), application specific integrated circuits (ASIC), discrete analog and digital circuits, and other circuitry. The system logic 414 is part of the implementation of any desired functionality in the example edge-zone device 132. In that regard, the system logic 414 may include logic that facilitates, as examples, decoding and playing music and video, e.g., MP3, MP4, MPEG, AVI, FLAC, AC3, or WAV decoding and playback; running applications; accepting user inputs; saving and retrieving application data; establishing, maintaining, and terminating cellular phone calls or data connections for, as one example, Internet connectivity; establishing, maintaining, and terminating wireless network connections, Bluetooth connections, or other connections; and displaying relevant information on the user interface 418. The user interface 418 and the inputs 428 may include a graphical user interface, touch sensitive display, haptic feedback or other haptic output, voice or facial recognition inputs, buttons, switches, speakers and other user interface elements. Additional examples of the inputs 428 include microphones, video and still image cameras, temperature sensors, vibration sensors, rotation and orientation sensors, headset and microphone input / output jacks, Universal Serial Bus (USB) connectors, memory card slots, radiation sensors (e.g., IR sensors), and other types of inputs.

[0042] The system logic 414 may include one or more processors 416 and memories 420. The memory 420 stores, for example, control instructions 422 that the processor 416 executes to carry out desired functionality for the example edge-zone device 132. The control parameters 424 provide and specify configuration and operating options for the control instructions 422. Further, the memory 420 may include a quarantined portfolio container 470, which may host various provisioned agents 472. The memory 420 may also store any BT, WiFi, 3G, 4G, 5G or other data that the edge-zone device 132 will send, or has received, through the communication interfaces 412.

[0043] In various implementations, the system power may be supplied by a power storage device, such as a battery 482.

[0044] In the communication interfaces 412, Radio Frequency (RF) transmit (Tx) and receive (Rx) circuitry 430 handles transmission and reception of signals through one or more antennas 432. The communication interface 412 may include one or more transceivers. The transceivers may be wireless transceivers that include modulation / demodulation circuitry, digital to analog converters (DACs), shaping tables, analog to digital converters (ADCs), filters, waveform shapers, filters, pre-amplifiers, power amplifiers and/or other logic for transmitting and receiving through one or more antennas, or (for some devices) through a physical (e.g., wireline) medium.

[0045] The transmitted and received signals may adhere to any of a diverse array of formats, protocols, modulations (e.g., QPSK, 16-QAM, 64-QAM, or 256-QAM), frequency channels, bit rates, and encodings. As one specific example, the communication interfaces 412 may include transceivers that support transmission and reception under the 2G, 3G, BT, WiFi, Universal Mobile Telecommunications System (UMTS), High Speed Packet Access (HSPA)+, and 4G / Long Term Evolution (LTE), and 5G standards. The techniques described below, however, are applicable to other wireless communications technologies whether arising from the 3rd Generation Partnership Project (3GPP), GSM Association, 3GPP2, IEEE, or other partnerships or standards bodies.

Example implementations

[0046] The following example implementations are described to be illustrative of various ones of the principles discussed above. However, the following examples are not intended to be limiting, but rather, in some cases, specific examples to aid in the illustration of the above described techniques and architectures. Various features of the following example implementations may be present in other implementations and absent in yet other implementations. The features of the following example implementations may be combined in various groupings in accord with the techniques and architectures described above.

[0047] Figure 5 shows an example ladder diagram 500 for an example system with a physically-localized edge-zone implementing various one of the techniques and architectures discussed above. In the example system, the agent provider may correspond to the display control prime, the agent store may correspond to the agent repository, the wallet may correspond to the portfolio container, and the "alt" box may define the physically-localized edge-zone. The "recommendations" may be displayed using pixel-state commands.

[0048] Figure 6 shows an example ladder diagram 600 for another example system with a logically-localized edge-zone implementing various one of the techniques and architectures discussed above. In the example system, the agent provider may correspond to the display control prime, the agent store may correspond to the agent repository, the wallet may correspond to the portfolio container, and the "alt" box may define the logically-localized edge-zone. The "recommendations" may be displayed using pixel-state commands.

[0049] The methods, devices, processing, and logic described above may be implemented in many different ways and in many different combinations of hardware and software. For example, all or parts of the implementations may be circuitry that includes an instruction processor, such as a Central Processing Unit (CPU), microcontroller, or a microprocessor; an Application Specific Integrated Circuit (ASIC), Programmable Logic Device (PLD), or Field Programmable Gate Array (FPGA); or

circuitry that includes discrete logic or other circuit components, including analog circuit components, digital circuit components or both; or any combination thereof. The circuitry may include discrete interconnected hardware components and/or may be combined on a single integrated circuit die, distributed among multiple integrated circuit dies, or implemented in a Multiple Chip Module (MCM) of multiple integrated circuit dies in a common package, as examples.

[0050] The circuitry may further include or access instructions for execution by the circuitry. The instructions may be embodied as a signal and/or data stream and/or may be stored in a tangible storage medium that is other than a transitory signal, such as a flash memory, a Random Access Memory (RAM), a Read Only Memory (ROM), an Erasable Programmable Read Only Memory (EPROM); or on a magnetic or optical disc, such as a Compact Disc Read Only Memory (CDROM), Hard Disk Drive (HDD), or other magnetic or optical disk; or in or on another machine-readable medium. A product, such as a computer program product, may particularly include a storage medium and instructions stored in or on the medium, and the instructions when executed by the circuitry in a device may cause the device to implement any of the processing described above or illustrated in the drawings.

[0051] The implementations may be distributed as circuitry, e.g., hardware, and/or a combination of hardware and software among multiple system components, such as among multiple processors and memories, optionally including multiple distributed processing systems. Parameters, databases, and other data structures may be separately stored and managed, may be incorporated into a single memory or database, may be logically and physically organized in many different ways, and may be implemented in many different ways, including as data structures such as linked lists, hash tables, arrays, records, objects, or implicit storage mechanisms. Programs may be parts (e.g., subroutines) of a single program, separate programs, distributed across several memories and processors, or implemented in many different ways, such as in a library, such as a shared library (e.g., a Dynamic Link Library (DLL)). The DLL, for example, may store instructions that perform any of the processing described above or illustrated in the drawings, when executed by the circuitry.

[0052] Various implementations may use the techniques and architectures described above.

[0053] E1. In an example useful for understanding the claimed invention, a product includes: machine-readable media other than a transitory signal; and instructions stored on the machine-readable media, the instructions configured to, when executed, cause a machine to: at network interface circuitry, establish a sanitized uplink between a privacy-secure-edge-zone provisioned agent and a central-zone-provisioned display control prime, the sanitized uplink configured to prevent upstream transport of un-sanitized data; and at control prime circuitry, exe-

cute a prime-blind open-loop pixel-state control of an edge-zone device by: providing a pixel-state control parameter matrix from the display control prime to the provisioned agent, the pixel-state control parameter matrix, the pixel-state control parameter matrix including multiple command-descriptors configured to support conditional prime command execution based on un-sanitized data, the display control prime being blind to the un-sanitized data; responsive to: the provisioned agent accessing the un-sanitized data while localized in the privacy-secure edge-zone; the provisioned agent determining, based on the pixel-state control parameter matrix and the un-sanitized data, an operative pixel-state command from among the command-descriptors; the provisioned agent causing a change to a pixel-state of the edge-zone device based on the operative pixel-state command; the provisioned agent receiving raw feedback input from a user interface of the edge-zone device responsive to the changed pixel-state; and the provisioned agent sanitizing the raw feedback input to generate sanitized feedback: receiving, at the display control prime in the central-zone, the sanitized feedback input from the provisioned agent via the sanitized uplink; and responsive to the sanitized feedback sending an unconditional pixel-state command configured to generate an acknowledgment pixel-state indicative of reception of the sanitized feedback.

[0054] E2. The product of example E1, where the provisioned agent is quarantined to a portfolio container while in the edge-zone.

[0055] E3. The product of example E2 or example E1, where the portfolio container is configured to enforce a sanitization criterion on the sanitized uplink.

[0056] E4. The product of either of examples E2 or E3 or example E1, where the portfolio container is configured to inspect incoming data on an import channel from memory controlled by the edge-zone device into the portfolio container.

[0057] Various implementations have been specifically described. However, many other implementations are also possible.

[0058] Headings and/or subheadings used herein are intended only to aid the reader with understanding described implementations.

Claims

1. A system including:

network interface circuitry configured to establish: a sanitized uplink (114) between a privacy-secure-edge-zone provisioned agent (134) and a central-zone-provisioned display control prime (112), the sanitized uplink configured to prevent upstream transport of un-sanitized data; and control prime circuitry configured to execute a prime-blind open-loop pixel-state control of an

edge-zone device by:

pre-provisioning the provisioned agent to a third-party-maintained agent repository to support provisioning on the edge-zone device;

providing a pixel-state control parameter matrix (118) from the display control prime to the provisioned agent by embedding the pixel-state control parameter matrix in the provisioned agent during pre-provisioning, the pixel-state control parameter matrix including multiple command-descriptors configured to support conditional prime command execution based on un-sanitized data, the display control prime being blind to the un-sanitized data;

responsive to:

the provisioned agent accessing (252) the un-sanitized data while localized in the privacy-secure edge-zone;

the provisioned agent determining, based on the pixel-state control parameter matrix and the un-sanitized data, an operative pixel-state command from among the command-descriptors;

the provisioned agent causing a change to a pixel-state of the edge-zone device based on the operative pixel-state command;

the provisioned agent receiving (256) raw feedback input from a user interface of the edge-zone device responsive to the changed pixel-state; and the provisioned agent sanitizing (258) the raw feedback input to generate sanitized feedback;

receiving, at the display control prime in the central-zone, the sanitized feedback from the provisioned agent via the sanitized uplink; and

responsive to the sanitized feedback sending, to the provisioned agent, an unconditional pixel-state command configured to generate an acknowledgement pixel-state indicative of reception of the sanitized feedback.

2. The system of claim 1, where the operative pixel-state command is configured to generate an interactive interface on a display of the edge-zone device.
3. The system of any one of the preceding claims, where the network interface circuitry is further configured to establish an edge-support downlink between the provisioned agent and the display control

prime.

4. The system of claim 3, where the control prime circuitry is configured to provide the pixel-state control parameter matrix by sending the pixel-state control parameter matrix to the provisioned agent via the edge-support downlink.

5. The system of any one of the preceding claims, where the provisioned agent is configured to comply with a pre-access condition before accessing the un-sanitized data.

6. The system of any one of the preceding claims, where the provisioned agent is quarantined to a portfolio container while in the edge-zone.

7. The system of claim 6, where the portfolio container is configured to enforce a sanitization criterion on the sanitized uplink.

8. The system of claim 6 or 7, where the portfolio container is configured to inspect incoming data on an import channel from memory controlled by the edge-zone device into the portfolio container.

9. The system of any one of the preceding claims, where the edge-zone includes a physically-localized region.

10. The system of any one of the preceding claims, where the edge-zone includes a logically localized region.

11. A method including:

at network interface circuitry, establishing a sanitized uplink (114) between a privacy-secure-edge-zone provisioned agent (134) and a central-zone-provisioned display control prime (112), the sanitized uplink configured to prevent upstream transport of un-sanitized data; and at control prime circuitry, executing a prime-blind open-loop pixel-state control of an edge-zone device by:

pre-provisioning the provisioned agent to a third-party-maintained agent repository to support provisioning on the edge-zone device;

providing a pixel-state control parameter matrix (118) from the display control prime to the provisioned agent by embedding the pixel-state control parameter matrix in the provisioned agent during pre-provisioning, the pixel-state control parameter matrix including multiple command-descriptors configured to support conditional prime com-

mand execution based on un-sanitized data, the display control prime being blind to the un-sanitized data;
responsive to:

the provisioned agent accessing (252) the un-sanitized data while localized in the privacy-secure edge-zone;
the provisioned agent determining, based on the pixel-state control parameter matrix and the un-sanitized data, an operative pixel-state command from among the command-descriptors;
the provisioned agent causing a change to a pixel-state of the edge-zone device based on the operative pixel-state command;
the provisioned agent receiving (256) raw feedback input from a user interface of the edge-zone device responsive to the changed pixel-state; and
the provisioned agent sanitizing (258) the raw feedback input to generate sanitized feedback:
receiving, at the display control prime in the central-zone, the sanitized feedback from the provisioned agent via the sanitized uplink; and

responsive to the sanitized feedback sending, to the provisioned agent, an unconditional pixel-state command configured to generate an acknowledgement pixel-state indicative of reception of the sanitized feedback.

12. The method of claim 11, where the operative pixel-state command is configured to generate an interactive interface on a display of the edge-zone device.

13. The method of claim 11 or 12, further including pre-provisioning the provisioned agent to a third-party-maintained agent repository to support provisioning on the edge-zone device.

Patentansprüche

1. System, umfassend:

eine Netzwerkschnittstellenschaltung, die dazu ausgestaltet ist, herzustellen: einen bereinigten Uplink (114) zwischen einem datenschutzsicheren provisionierten Mittel (134) im Randbereich und einem provisionierten Anzeigesteuerungsprime (112) im Mittelbereich, wobei der bereinigte Uplink dazu ausgestaltet ist, eine vorge-schaltete Übermittlung von unbereinigten Daten

zu verhindern; und
eine Steuerprimeschaltung, die dazu ausgestaltet ist, eine prime-blinde offenkreisige Pixelzustandssteuerung einer Randbereichsvorrichtung durch Folgendes auszuführen:

vorab Provisionieren des provisionierten Mittels an ein von einer Drittpartei verwaltetes Mitteldepot, um ein Provisionieren auf der Randbereichsvorrichtung zu unterstützen;
Bereitstellen einer Steuerparametermatrix (118) im Pixelzustand von dem Anzeigesteuerungsprime für das provisionierte Mittel durch Einbetten der Steuerparametermatrix im Pixelzustand in das provisionierte Mittel während des Provisionierens vorab, wobei die Steuerparametermatrix im Pixelzustand mehrere Befehlsdeskriptoren umfasst, die dazu ausgestaltet sind, eine bedingte Primebefehlsausführung basierend auf unbereinigten Daten zu unterstützen, wobei das Anzeigesteuerungsprime blind für die unbereinigten Daten ist;
ansprechend darauf, dass:

das provisionierte Mittel auf die unbereinigten Daten zugreift (252), während es in dem datenschutzsicheren Randbereich lokalisiert ist;

das provisionierte Mittel, basierend auf der Steuerparametermatrix im Pixelzustand und den unbereinigten Daten, einen operativen Pixelzustandsbefehl aus den Befehlsdeskriptoren bestimmt; das provisionierte Mittel eine Änderung an einem Pixelzustand der Randbereichsvorrichtung basierend auf dem operativen Pixelzustandsbefehl verursacht;

das provisionierte Mittel rohe Rückkopplungseingaben von einer Nutzerschnittstelle der Randbereichsvorrichtung ansprechend auf den geänderten Pixelzustand empfängt (256); und
das provisionierte Mittel die rohen Rückkopplungseingaben bereinigt (258), um eine bereinigte Rückkopplung zu erzeugen:

Empfangen, an dem Anzeigesteuerungsprime im Mittelbereich, der bereinigten Rückkopplung von dem provisionierten Mittel über den bereinigten Uplink; und

ansprechend auf die bereinigte Rückkopplung, Senden, an das provisionierte Mittel, eines bedingungslosen Pixelzustandsbe-

- fehls, der dazu ausgestaltet ist, einen Bestätigungspixelzustand zu erzeugen, der auf einen Empfang der bereinigten Rückkopplung hinweist.
2. System nach Anspruch 1, wobei der operative Pixelzustandsbefehl dazu ausgestaltet ist, eine interaktive Schnittstelle auf einer Anzeige der Randbereichsvorrichtung zu erzeugen.
3. System nach einem der vorhergehenden Ansprüche, wobei die Netzwerkschnittstellenschaltung ferner dazu ausgestaltet ist, einen Randunterstützungsdowlink zwischen dem provisionierten Mittel und dem Anzeigesteuerungsprime herzustellen.
4. System nach Anspruch 3, wobei die Steuerprimeschaltung dazu ausgestaltet ist, die Steuerparametermatrix im Pixelzustand durch Senden der Steuerparametermatrix im Pixelzustand an das provisionierte Mittel über den Randunterstützungsdowlink bereitzustellen.
5. System nach einem der vorhergehenden Ansprüche, wobei das provisionierte Mittel dazu ausgestaltet ist, eine Vorzugsbedingung zu erfüllen, bevor auf die unbereinigten Daten zugegriffen wird.
6. System nach einem der vorhergehenden Ansprüche, wobei das provisionierte Mittel in einen Portfoliobehälter isoliert wird, während es im Randbereich ist.
7. System nach Anspruch 6, wobei der Portfoliobehälter dazu ausgestaltet ist, ein Bereinigungskriterium an dem bereinigten Uplink durchzusetzen.
8. System nach Anspruch 6 oder 7, wobei der Portfoliobehälter dazu ausgestaltet ist, eingehende Daten auf einem Importkanal aus einem Speicher, der von der Randbereichsvorrichtung gesteuert wird, in den Portfoliobehälter zu überprüfen.
9. System nach einem der vorhergehenden Ansprüche, wobei der Randbereich einen physisch lokalisierten Bereich umfasst.
10. System nach einem der vorhergehenden Ansprüche, wobei der Randbereich einen logisch lokalisierten Bereich umfasst.
11. Verfahren, umfassend:
- an einer Netzwerkschnittstellenschaltung, Herstellen eines bereinigten Uplinks (114) zwischen einem datenschutzsicheren provisionierten Mittel (134) im Randbereich und einem provisionierten Anzeigesteuerungsprime (112) im Mit-

telbereich, wobei der bereinigte Uplink dazu ausgestaltet ist, eine vorgeschaltete Übermittlung von unbereinigten Daten zu verhindern; und

an einer Steuerprimeschaltung, Ausführen einer prime-blinden offenkreisigen Pixelzustandssteuerung einer Randbereichsvorrichtung durch:

vorab Provisionieren des provisionierten Mittels an ein von einer Drittpartei verwaltetes Mitteldepot, um ein Provisionieren auf der Randbereichsvorrichtung zu unterstützen;

Bereitstellen einer Steuerparametermatrix (118) im Pixelzustand von dem Anzeigesteuerungsprime für das provisionierte Mittel durch Einbetten der Steuerparametermatrix im Pixelzustand in das provisionierte Mittel während des Provisionierens vorab, wobei die Steuerparametermatrix im Pixelzustand mehrere Befehlsdeskriptoren umfasst, die dazu ausgestaltet sind, eine bedingte Primebefehlsausführung basierend auf unbereinigten Daten zu unterstützen, wobei das Anzeigesteuerungsprime blind für die unbereinigten Daten ist; ansprechend darauf, dass:

das provisionierte Mittel auf die unbereinigten Daten zugreift (252), während es in dem datenschutzsicheren Randbereich lokalisiert ist;

das provisionierte Mittel, basierend auf der Steuerparametermatrix im Pixelzustand und den unbereinigten Daten, einen operativen Pixelzustandsbefehl aus den Befehlsdeskriptoren bestimmt; das provisionierte Mittel eine Änderung an einem Pixelzustand der Randbereichsvorrichtung basierend auf dem operativen Pixelzustandsbefehl verursacht;

das provisionierte Mittel rohe Rückkopplungseingaben von einer Nutzerschnittstelle der Randbereichsvorrichtung ansprechend auf den geänderten Pixelzustand empfängt (256); und das provisionierte Mittel die rohen Rückkopplungseingaben bereinigt (258), um eine bereinigte Rückkopplung zu erzeugen:

Empfangen, an dem Anzeigesteuerungsprime im Mittelbereich, der bereinigten Rückkopplung von dem provisionierten Mittel über den bereinigten Uplink; und

ansprechend auf die bereinigte Rückkopplung, Senden, an das provisionierte Mittel, eines bedingungslosen Pixelzustandsbefehls, der dazu ausgestaltet ist, einen Bestätigungspixelzustand zu erzeugen, der auf einen Empfang der bereinigten Rückkopplung hinweist.

12. Verfahren nach Anspruch 11, wobei der operative Pixelzustandsbefehl dazu ausgestaltet ist, eine interaktive Schnittstelle auf einer Anzeige der Randbereichsvorrichtung zu erzeugen.
13. Verfahren nach Anspruch 11 oder 12, ferner umfassend vorab Provisionieren des provisionierten Mittels an ein von einer Drittpartei verwaltetes Mitteldepot, um ein Provisionieren auf der Randbereichsvorrichtung zu unterstützen.

Revendications

1. Système comportant :

des circuits d'interface réseau configurés pour établir : une liaison montante assainie (114) entre un agent provisionné de zone périphérique à confidentialité sécurisée (134) et un primaire de contrôle d'affichage provisionné de zone centrale (112), la liaison montante assainie étant configurée pour empêcher le transport en amont de données non assainies ; et des circuits primaires de contrôle configurés pour exécuter un contrôle d'état de pixel en boucle ouverte invisible au primaire d'un dispositif de zone périphérique par :

le pré-provisionnement de l'agent provisionné sur un référentiel maintenu par un tiers pour prendre en charge le provisionnement sur le dispositif de zone périphérique ; la fourniture d'une matrice de paramètres de contrôle d'état de pixel (118) en provenance du primaire de contrôle d'affichage à l'agent provisionné en intégrant la matrice de paramètres de contrôle d'état de pixel à l'agent provisionné pendant le pré-provisionnement, la matrice de paramètres de contrôle d'état de pixel comportant de multiples descripteurs de commande configurés pour prendre en charge une exécution conditionnelle de commande de primaire sur la base de données non assainies, le primaire de contrôle d'affichage étant aveugle aux données non assainies ; en réponse à :

l'accès (252) par l'agent provisionné aux données non assainies pendant qu'il est localisé dans la zone périphérique à confidentialité sécurisée ; la détermination par l'agent provisionné, sur la base de la matrice de paramètres de contrôle d'état de pixel et des données non assainies, d'une commande opérationnelle d'état de pixel parmi les descripteurs de commande ; au déclenchement par l'agent provisionné d'une modification d'un état de pixel du dispositif de zone périphérique sur la base de la commande opérationnelle d'état de pixel ; à la réception (256) par l'agent provisionné d'une entrée de retour brute en provenance d'une interface d'utilisateur du dispositif de zone périphérique en réponse à l'état de pixel modifié ; et à l'assainissement (258) par l'agent provisionné de l'entrée de retour brute pour générer un retour assaini :

la réception, au niveau du primaire de contrôle d'affichage dans la zone centrale, du retour assaini en provenance de l'agent provisionné par l'intermédiaire de la liaison montante assainie ; et en réponse au retour assaini, la transmission, à l'agent provisionné, d'une commande inconditionnelle d'état de pixel configurée pour générer un état de pixel d'accusé de réception indiquant la réception du retour assaini.

2. Système selon la revendication 1, dans lequel la commande opérationnelle d'état de pixel est configurée pour générer une interface interactive sur un afficheur du dispositif de zone périphérique.
3. Système selon l'une quelconque des revendications précédentes, dans lequel les circuits d'interface réseau sont en outre configurés pour établir une liaison descendante de prise en charge de périphérie entre l'agent provisionné et le primaire de contrôle d'affichage.
4. Système selon la revendication 3, dans lequel les circuits primaires de contrôle sont configurés pour fournir la matrice de paramètres de contrôle d'état de pixel en transmettant la matrice de paramètres de contrôle d'état de pixel à l'agent provisionné par l'intermédiaire de la liaison descendante de prise en charge de périphérie.

5. Système selon l'une quelconque des revendications précédentes, dans lequel l'agent provisionné est configuré pour satisfaire à une condition de pré-ac-
cès avant d'accéder aux données non assainies. 5
6. Système selon l'une quelconque des revendications précédentes, dans lequel l'agent provisionné est confiné à un conteneur de portefeuille pendant qu'il est dans la zone périphérique. 10
7. Système selon la revendication 6, dans lequel le conteneur de portefeuille est configuré pour appliquer un critère d'assainissement à la liaison montante assainie. 15
8. Système selon la revendication 6 ou 7, dans lequel le conteneur de portefeuille est configuré pour inspecter des données entrantes sur un canal d'importation en provenance d'une mémoire contrôlée par le dispositif de zone périphérique vers le conteneur de portefeuille. 20
9. Système selon l'une quelconque des revendications précédentes, dans lequel la zone périphérique comporte une région localisée physiquement. 25
10. Système selon l'une quelconque des revendications précédentes, dans lequel la zone périphérique comporte une région localisée logiquement. 30
11. Procédé, comportant :
 - au niveau de circuits d'interface réseau, l'établissement d'une liaison montante assainie (114) entre un agent provisionné de zone périphérique à confidentialité sécurisée (134) et un primaire de contrôle d'affichage provisionné de zone centrale (112), la liaison montante assainie étant configurée pour empêcher le transport en amont de données non assainies ; et 35
 - au niveau de circuits primaires de contrôle, l'exécution d'un contrôle d'état de pixel en boucle ouverte invisible au primaire d'un dispositif de zone périphérique par : 40
 - le pré-provisionnement de l'agent provisionné sur un référentiel maintenu par un tiers pour prendre en charge le provisionnement sur le dispositif de zone périphérique ; 45
 - la fourniture d'une matrice de paramètres de contrôle d'état de pixel (118) en provenance du primaire de contrôle d'affichage à l'agent provisionné en intégrant la matrice de paramètres de contrôle d'état de pixel à l'agent provisionné pendant le pré-provisionnement, la matrice de paramètres de contrôle d'état de pixel comportant de mul-

tiples descripteurs de commande configurés pour prendre en charge une exécution conditionnelle de commande de primaire sur la base de données non assainies, le primaire de contrôle d'affichage étant aveugle aux données non assainies ;
en réponse à :

l'accès (252) par l'agent provisionné aux données non assainies pendant qu'il est localisé dans la zone périphérique à confidentialité sécurisée ;
la détermination par l'agent provisionné, sur la base de la matrice de paramètres de contrôle d'état de pixel et des données non assainies, d'une commande opérationnelle d'état de pixel parmi les descripteurs de commande ;
au déclenchement par l'agent provisionné d'une modification d'un état de pixel du dispositif de zone périphérique sur la base de la commande opérationnelle d'état de pixel ;
à la réception (256) par l'agent provisionné d'une entrée de retour brute en provenance d'une interface d'utilisateur du dispositif de zone périphérique en réponse à l'état de pixel modifié ;
et
à l'assainissement (258) par l'agent provisionné de l'entrée de retour brute pour générer un retour assaini :

la réception, au niveau du primaire de contrôle d'affichage dans la zone centrale, du retour assaini en provenance de l'agent provisionné par l'intermédiaire de la liaison montante assainie ; et
en réponse au retour assaini, la transmission, à l'agent provisionné, d'une commande inconditionnelle d'état de pixel configurée pour générer un état de pixel d'accusé de réception indiquant la réception du retour assaini.

12. Procédé selon la revendication 11, dans lequel, la commande opérationnelle d'état de pixel est configurée pour générer une interface interactive sur un afficheur du dispositif de zone périphérique. 50
13. Procédé selon la revendication 11 ou 12, comportant en outre le pré-provisionnement de l'agent provisionné sur un référentiel maintenu par un tiers pour prendre en charge le provisionnement sur le dispositif de zone périphérique. 55

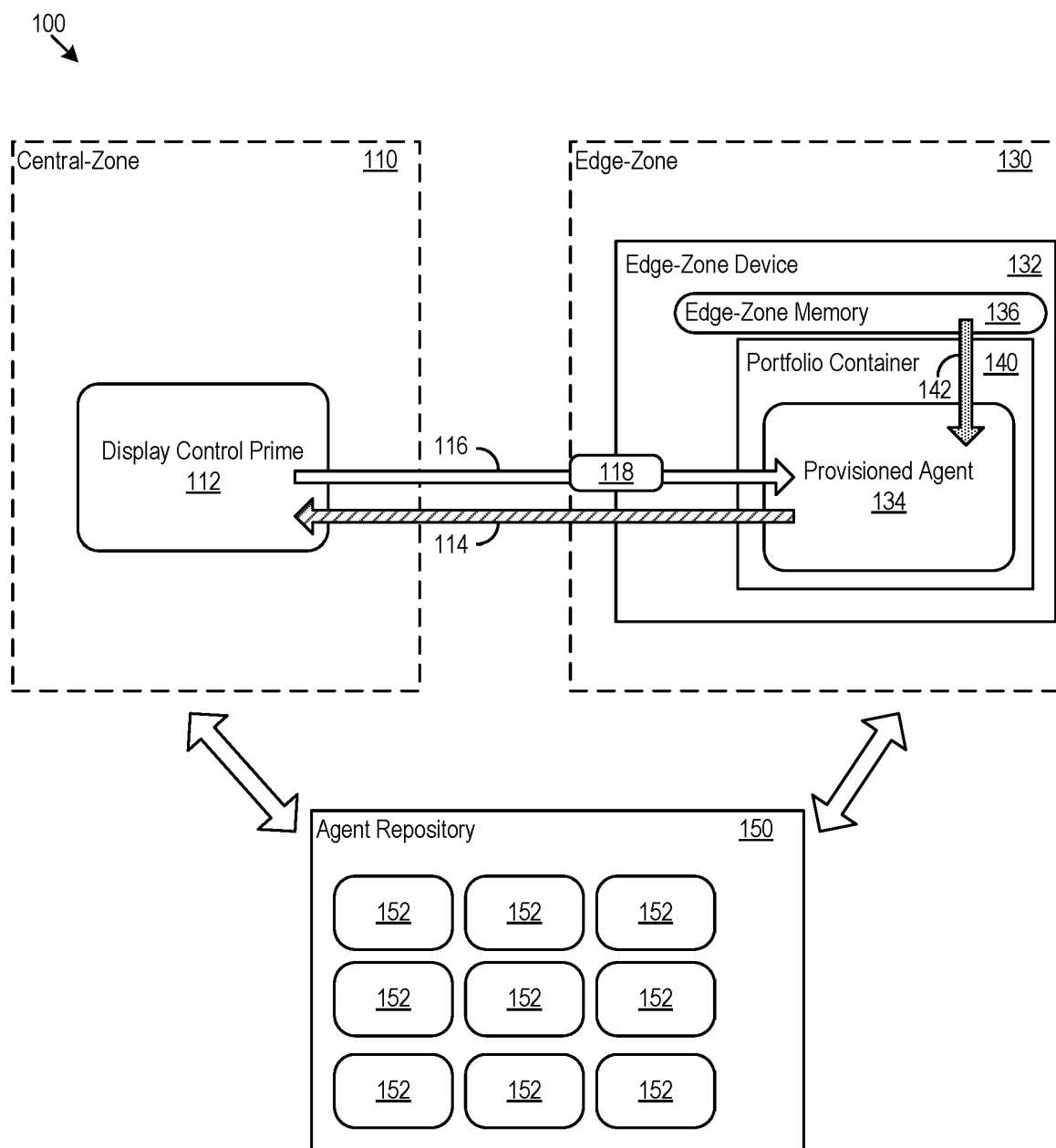


Figure 1

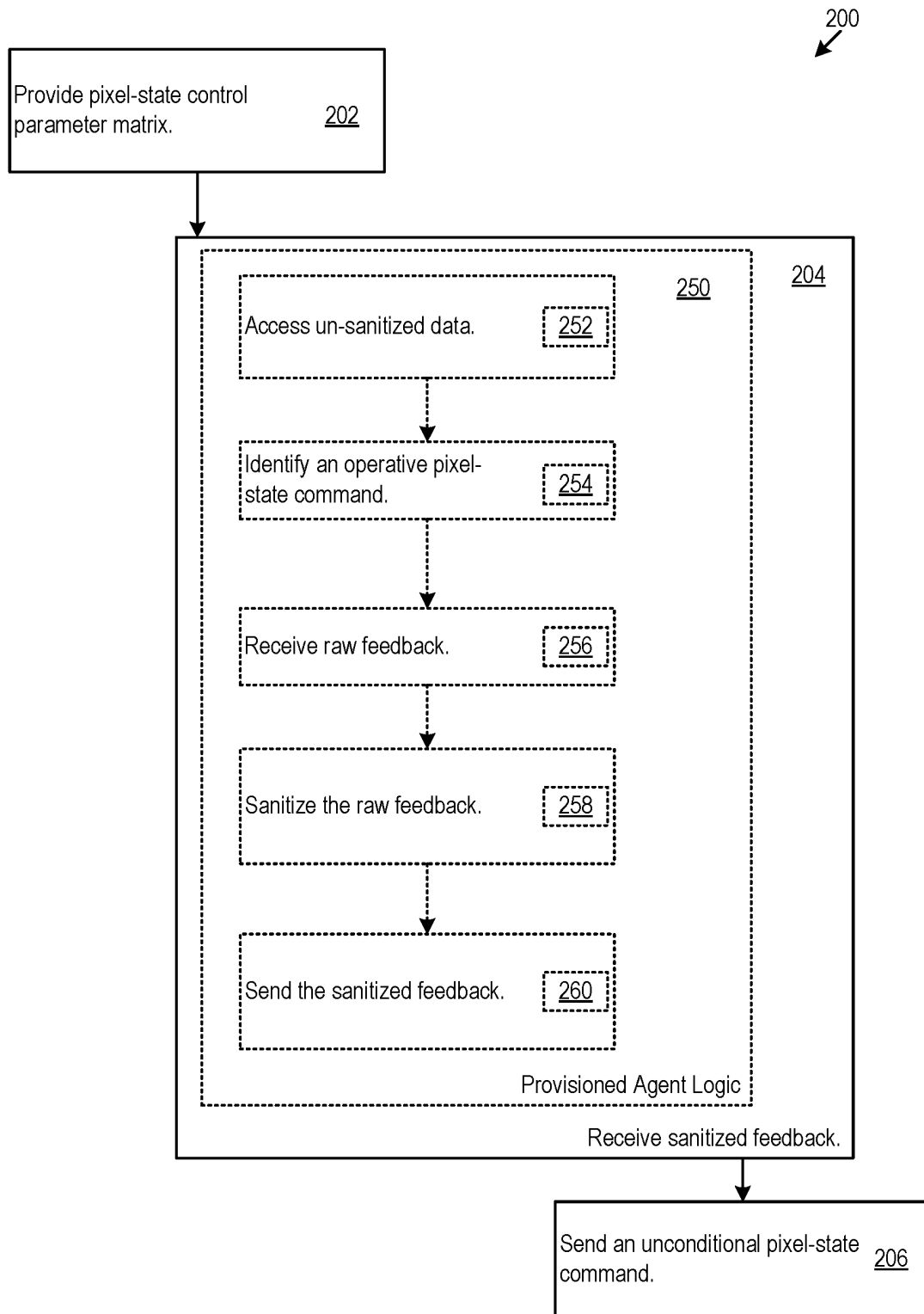


Figure 2

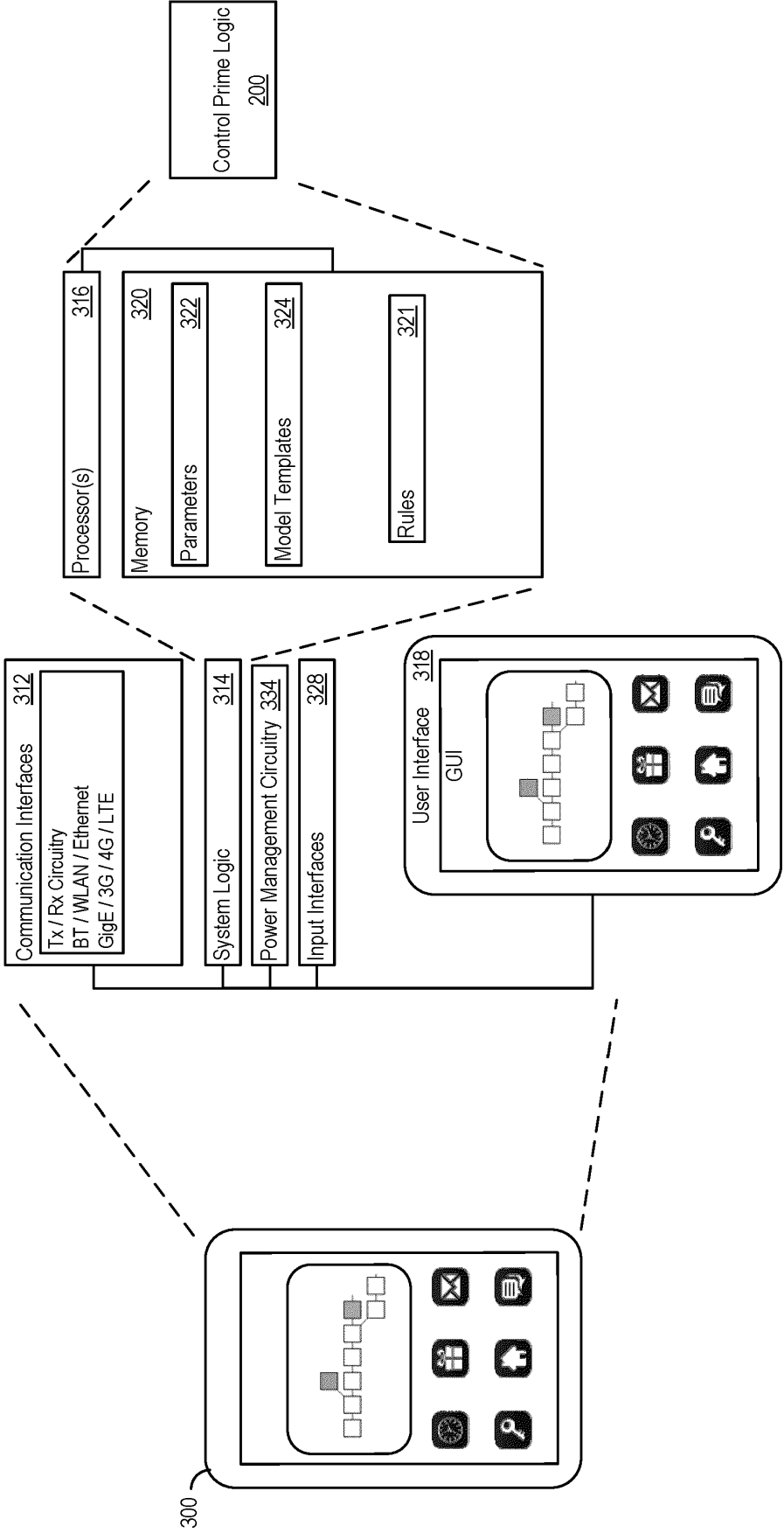


Figure 3

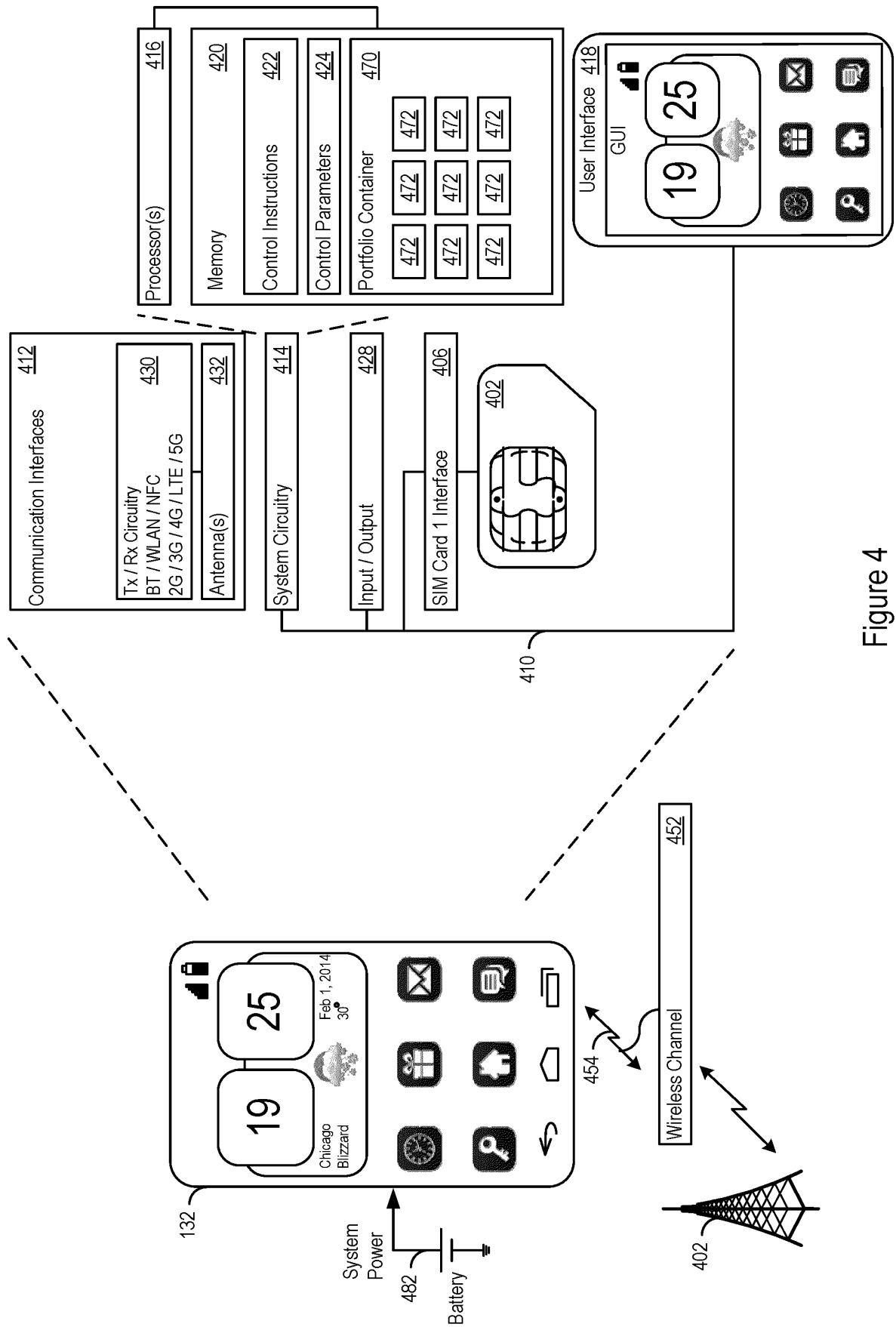


Figure 4

500

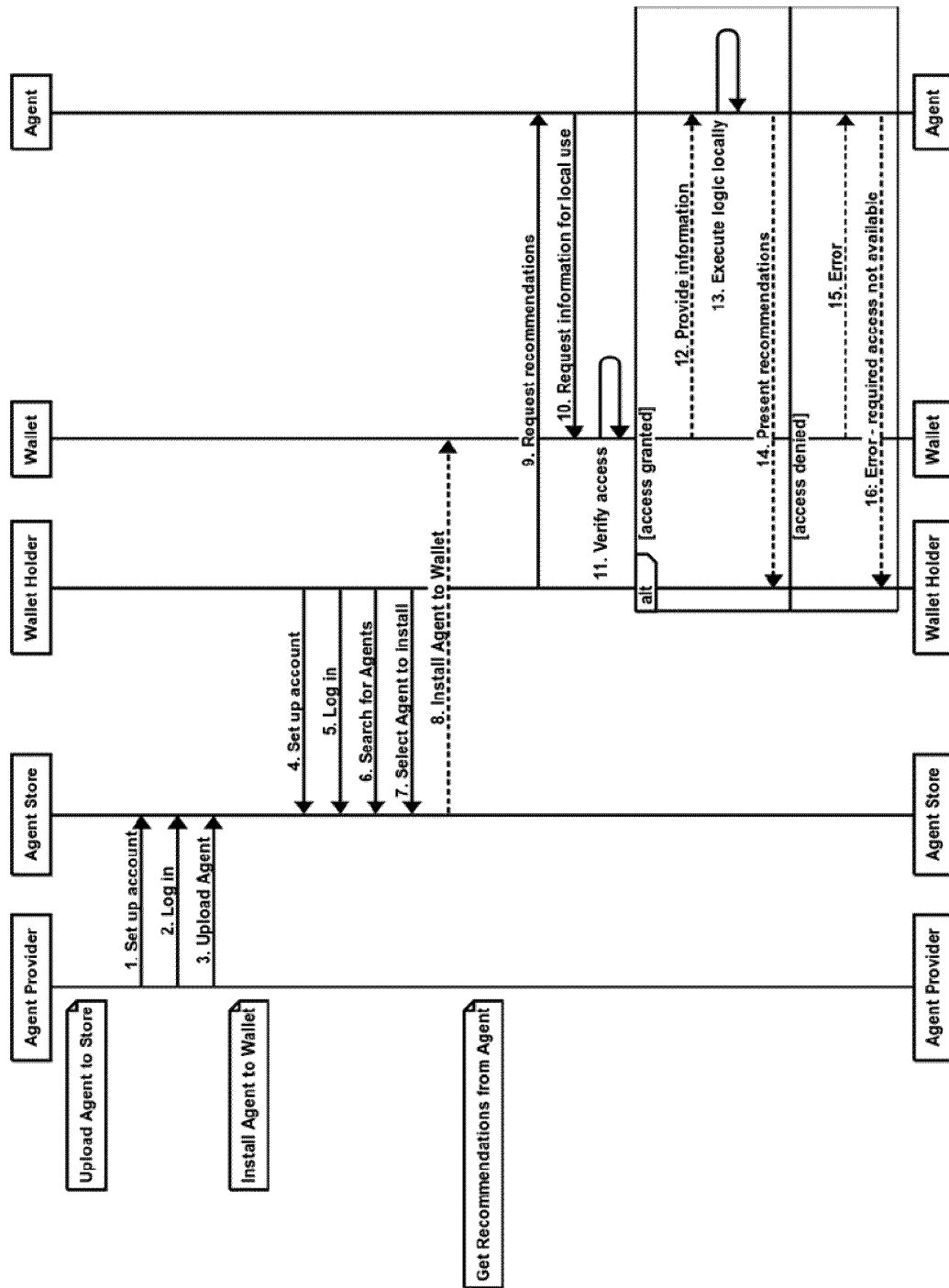


Figure 5

600 ↗

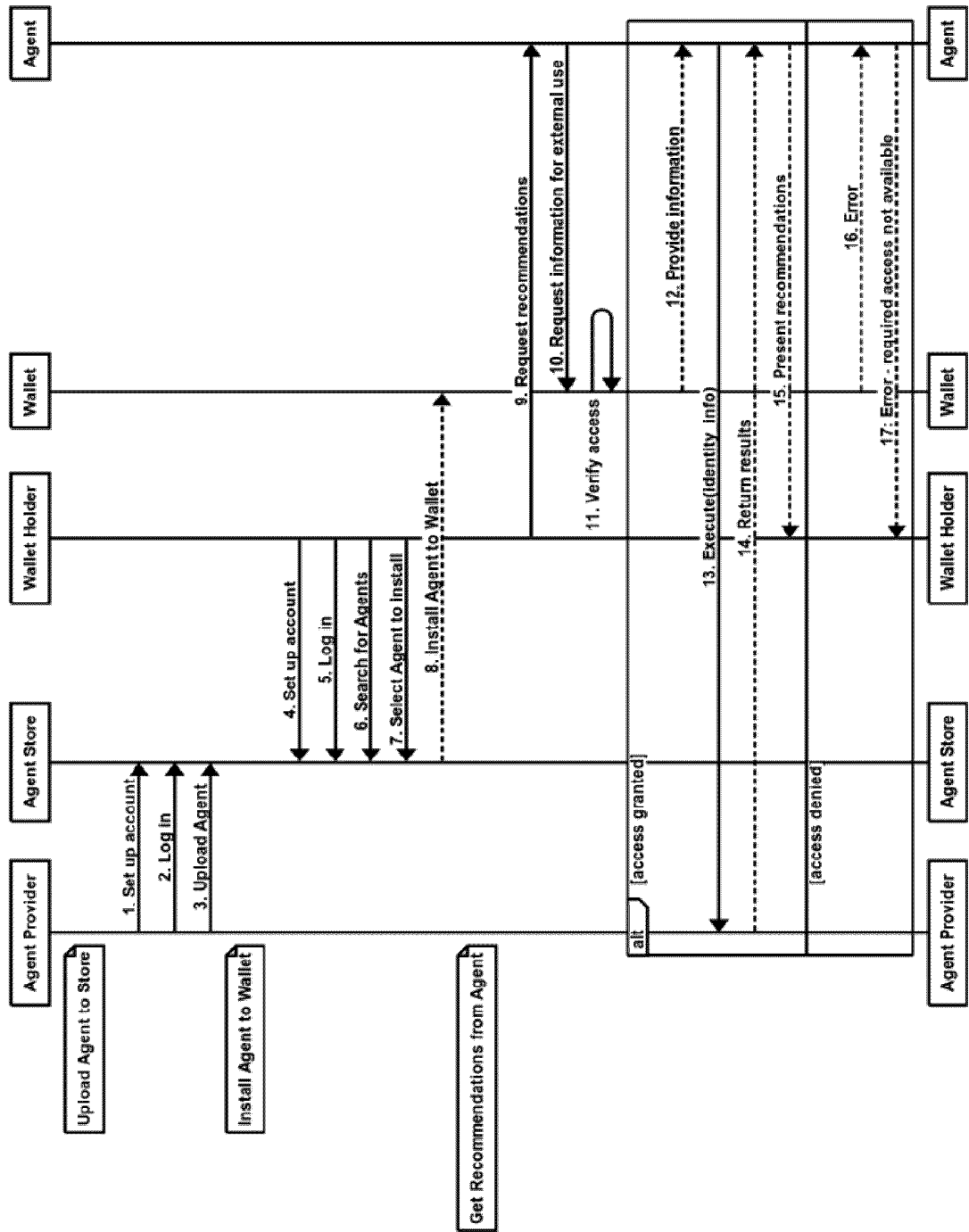


Figure 6

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 88198920 [0001]
- US 62910079 [0001]
- US 20170039389 A1 [0004]
- US 20160006754 A1 [0005]
- WO 2012118870 A1 [0006]